REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims **1-37** are pending in the application.

Claims **1-37** have been rejected.

Claims **1**, **21**, **26**, **32** and **34** have been amended in this submission. Applicants respectfully assert that the amendments to the claims add no new matter.

Examiner Interview

Initially, Applicants wish to thank Examiner Anderson for granting and conducting the in-person interview of December 6, 2011 with Applicants' representative, Guy Yonay (Reg. No. 52,388). In the interview, Applicants' representatives pointed out that the Richmond reference is directed to managing access to network resources, in contrast, the present invention as claimed is directed to controlling a transfer of data between a computer and an external device connected to a physical port of the computer.

CLAIM REJECTIONS

35 U.S.C. § 102 Rejections

In the final Office action, the Examiner rejected claims 1-37 under 35 U.S.C. § 102(b), as being anticipated by Richmond et al. (U.S. Pat. Pub. No. 2003/0154380) ("Richmond"). Applicants respectfully traverse this rejection at least in view of the remarks that follow.

Richmond is directed to controlling usage of network resources but is unrelated to protecting, managing or controlling transfer of information between a computer and an external device connected to a physical port of the computer.

As taught by Richmond, an entry point device such as a switch or hub controls usage of network resources by a user.

> Usage of network resources of a communications network by a user beyond a network device of the communications network that serves as the user's entry point to the communications network is controlled. The port module of the network device is configured with one or more packet rules corresponding to an identity of the user. A packet is received from a device used by the user at the port module, and, before using any of the network resources beyond the network device, the one or more packet rules are applied to the received packet. (Richmond, Abstract, emphasis added).

In contrast, the invention as claimed is directed to controlling a transfer of data between a computer and an external device connected to a physical port of the computer.

> Security agent 230 may be activated when a physical communication port is requested. The security agent 230 may pull the transportation to and from the physical communication port, processes the information and may reach a decision regarding the legality of the requested connection and/or data transfer. (Application as filed, para. [0041], emphasis added).

Accordingly, the invention as claimed and the Richmond reference are directed to different fields and solve different problems. In fact, controlling a transfer of information between a computer and an external device connected to physical port of the computer would serve no purpose to Richmond which is directed to controlling usage of

network resources but is unrelated to controlling the transfer of data between a computer and an external device connected to a port of the computer (e.g., a data storage device).

To further clarify the scope of the invention, Applicants have amended claim 1 to recite "receiving, by a module on the computer, a data portion of a file being communicated during a data communication session between the computer and a removable external device, said removable external device connected to a physical communication port of the computer" (emphasis added).

Support for the amendment of claim 1 may be found throughout the application, for example:

> Internal employees may use their permission to gain access to the enterprise's information, download the information to their client computer and then transfer the information to an external device. The external device may be a removable storage device (e.g. flash memory, such as but not limited to, DiscOnKey or a removable hard disk drive), a removable storage media (e.g., floppy disk or writable CD ROM), a PDA, a cellular phone, WiFi dongle, MP3 player, Bluetooth dongle, printer, digital camera, tokens, etc. [...] Communication with such external devices may be done over a variety of data communication physical ports such as USB, FireWire, PCMCIA bus, SCSI bus, iSCSI, Cellular, Infiniband, Serial, Parallel, LAN port, Fiber Channel, Infrared, wireless communication such as but not limited WiFi, Bluetooth, etc. (Application as filed, para. [0006], emphasis added).
>
> * * *
>
> Thus, the portable memory can be used as a digital camera for loading information into a computer but any attempt to transfer files to the portable memory will be thwarted. (Application as filed, para. [0015], emphasis added).
>
> * * *
>
> For example, this may occur under the scenario in which the application is "Write" to a DiskOnKey and the security policy requires checking of "Water Marks" in the content of the file. In this scenario, the MDM 320 may wait until the entire content of the file has been analyzed. "Water Marks" are "undetectable" digital images with 8 bit gray scales. (Application as filed, para. [0079], emphasis added).

Richmond is directed to controlling usage of network resources by a user at the user's entry point to a communications network. As disclosed by Richmond, packet rules are applied before usage of a network is allowed:

> Packet rules may be provisioned to the user's entry point to the network, and the packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used. (Richmond, Abstract, emphasis added).

However, once access to a network resource is allowed, Richmond has no use for further inspection of data being transferred. Accordingly, Richmond does not teach receiving a data portion of a file being communicated, buffering portions of the file, analyzing data portions and/or determining, based on the analysis, whether to allow a data communication session because, as taught by Richmond, a decision on whether or not to allow a session is reached before actual data is being transferred.

On page 3 of the final Office action, in the response to arguments (section b), the Examiner stated that Richmond teaches analyzing data according to a protocol associated with a physical port of the computer, Applicants respectfully disagree. Paragraph [0048] of Richmond discloses:

> In another aspect of this embodiment, the rule application logic is operative to apply the one or more packet rules to all packets received from the device of the user at the port module until the user logs off of the communications network. (emphasis added)

Clearly, applying packet rules to all packets received from a user does not amount to analyzing data according to a protocol associated with a physical port of a computer. Related to packets received from a user, processing of packets as taught by Richmond is unrelated to a physical port of a computer. Accordingly, applicants submit this element is not taught by Richmond.

In the response to arguments (section c), the Examiner stated that Richmond teaches storing a portion of data communicated between a computer and an external device pointing to Fig. 3/item 308 and Fig. 4/item 410.

However, storing a relationship hierarchy as shown by 308 in Fig. 3 (and item 410 in Fig. 4) of Richmond is unrelated to storing a data portion of a file being communicated during a data communication session between a computer and a removable external device connected to a physical communication port of the computer as recited by amended claim 1. Richmond teaches storing a relationship hierarchy:

> The relationship hierarchy 200 may include one or more roles 202-206, one or more service abstractions 208-214 and one or more packet rules 220-231. (Richmond, para. [0099], emphasis added).

However, Richmond clearly does not teach storing a portion of a file being communicated. Rather, rules, service abstractions and other information related to communicated data are stored. Applicants note that storing information related to the data communicated (such as rules or roles) is not to be confused with storing a portion of a file being communicated or transferred.

In the response to arguments (section d), the Examiner stated that Richmond teaches modifying the type of the transportation, the status of a requested file and correcting the data pointing to a network administrator that may configure/modify a packet rule.

First, modifying a packet rule (or any other rule for that matter) does not amount to modifying a type of a transportation, modifying a status of a requested file or correcting a data as claimed.

Second, as claimed, the above operations are performed by a module on the computer. Clearly, by teaching an administrator to manually configure rules, Richmond does not teach a module on a computer to modify a type of a transportation, modify a status of a requested file or correct data being transferred.

In light of the above discussion, independent claim 1 as amended is allowable over Richmond. The discussion above is relevant to independent claims 21 and 34 which have been amended to recite similar elements and are therefore allowable over Richmond.

Each of dependent claims 2-19, 22-33 and 35-37 depends, directly or indirectly, from one of independent claims 1, 21 and 34 and includes all the features of the claim from which it depends as well as additional distinguishing features, and is therefore allowable. Accordingly, claims 2-19, 22-33 and 35-37 are allowable over Richmond.

In view of the foregoing amendments and remarks, Applicants assert that the pending claims are allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

Please charge any fees associated with this paper to deposit account No. 50-3355.

Respectfully submitted,

/Guy Yonay/
Guy Yonay
Attorney/Agent for Applicants
Registration No. 52,388
Dated: December 28, 2011

Pearl Cohen Zedek Latzer, LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801